File No. 44

House Bill No. 5394

House of Representatives, March 16, 1998. The Committee on Government Administration and Elections reported through REP. BYSIEWICZ, 100th DIST., Chairman of the Committee on the part of the House, that the bill ought to pass.

AN ACT ESTABLISHING A VOLUNTARY BUSINESS CODE FOR THE PROTECTION OF PERSONAL INFORMATION.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) As used in this section and sections 2 to 4, inclusive, of this act:

(1) "Personal information" means recorded information about an identifiable individual, including, but not limited to:

(A) Information relating to the race, national or ethnic origin, color, religion, age, sex, sexual orientation or marital or family status of the individual;

(B) Information relating to the education or the medical, psychiatric, psychological, criminal nonconviction or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(C) Any identifying number, symbol or other particular assigned to the individual;

(D) The address, telephone number, fingerprints or blood type of the individual;

(E) Correspondence sent to a business by the individual that is of a private or confidential nature, and responses by the business to such

correspondence that would reveal the contents of the correspondence; and

(F) The individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

(2) "Business" means any for-profit or nonprofit organization or entity, including a sole proprietorship, which collects, records, maintains, discloses or disseminates personal information. "Business" shall not include (A) a human being who is not a sole proprietorship or (B) a public agency, as defined in section 1-18a of the general statutes, as amended by section 1 of public act 97-47.

(3) "Personal information system" means a collection of records containing personal information.

Sec. 2. (NEW) A business shall be eligible for certification under section 4 of this act if it complies with the following Voluntary Code for the Protection of Personal Information, by agreeing to:

(1) (A) Inform each of its employees who operates or maintains a personal information system or who has access to personal information (i) of the provisions of this section and procedures adopted under this section, and (ii) any applicable state or federal law or regulations concerning maintenance or disclosure of personal information kept by the business;

(B) Designate an employee or employees who are accountable for the business's compliance with the provisions of this section and disclose the identity of such employee or employees upon request; and

(C) Be responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing;

(2) Take reasonable precautions to protect personal information from the dangers of (A) fire, flood, natural disaster or other physical threats, (B) theft or loss, and (C) unauthorized access, disclosure, copying, use or modification;

(3) (A) Obtain the consent of an individual before collecting, using or disclosing personal

information concerning the individual, except when (i) legal, medical or security reasons make it impossible or impractical to seek consent, (ii) information is being collected for the detection and prevention of fraud or for law enforcement, (iii) seeking consent is impossible or inappropriate when the individual is a minor, seriously ill or mentally incapacitated, (iv) the business is not able to seek consent because it does not have a direct relationship with the individual, (v) the collection, use or disclosure of personal information without the individual's consent is authorized by state or federal law or is required pursuant to a subpoena, court order or other judicial process, (vi) such collection, use or disclosure of the information is necessary for the performance of a contract to which the individual is a party or in order to take steps at the request of the individual prior to entering into a contract, (vii) such collection, use or disclosure is necessary to protect the vital interests of the individual, (viii) such collection, use or disclosure is necessary for the performance of a task carried out in the public interest, or (ix) such collection, use or disclosure is for the legitimate interests of the business except (I) in the case of personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership and information concerning health or sex life and (II) in the case of any other personal information such legitimate interests are overridden by the fundamental rights and freedoms of natural persons and in particular their right to privacy;

(B) (i) Obtain the consent of an individual before using or disclosing personal information for purposes other than those for which it was collected, subject to the same exceptions in subparagraph (A) of this subdivision, and (ii) destroy, erase or make anonymous personal information that is no longer needed to fulfil the identified purposes;

(4) Maintain only that information about an individual which is relevant and necessary to accomplish the purposes of the business and identify such purposes at or before the time that the information is collected;

(5) Make readily available to an individual specific information about the business's policies and practices relating to the management of personal information;

(6) Upon a written request, inform an individual, in writing, whether the business maintains personal information concerning him;

(7) Upon a written request, disclose to an individual, on a plain language form, all personal information concerning him which is maintained by the business. The provisions of this subdivision shall be subject to the provisions of section 4-194 of the general statutes, except that "agency" in said section 4-194 shall be deemed to mean such business. If disclosure of personal information is made under this subdivision, the business shall not disclose any personal information concerning individuals other than the requesting individual;

(8) Establish procedures which:

(A) Allow an individual to contest the accuracy, completeness or relevancy of his personal information;

(B) Allow personal information to be corrected upon request of an individual when the business concurs in the proposed correction;

(C) Allow an individual who believes that the business maintains inaccurate or incomplete personal information concerning him to add a statement to the personal information system, setting forth what he believes to be an accurate or complete version of such personal information. Such a statement (i) shall become and remain a part of the business's personal information system, until such personal information is deleted from the system, and (ii) shall be disclosed to any person, agency or organization to which the disputed personal information is disclosed;

(9) Upon a written request, provide the following information to an individual from whom or about whom personal information is collected: (A) The identity of the employee or employees designated under subparagraph (B) of subdivision (1) of this section to be accountable for the business's compliance with the provisions of this section; (B) the intended purposes for the collection, use or disclosure of the information; and (C) the recipients of any information

disclosed, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of the right of access to and the right to rectify the information. The provisions of this subdivision shall not apply if the information is obtained from a third party and disclosure of the information described in subparagraphs (A), (B) and (C) of this subdivision is impossible or would involve a disproportionate effort; and

(10) Grant an individual from whom or about whom personal information is collected the right to object at any time on compelling legitimate grounds relating to the individual's particular situation to the collection, use or disclosure of such information.

Sec. 3. (a) There is established a Personal Information Standards Commission.

(b) The commission shall consist of the following members:

(1) Two appointed by the speaker of the House of Representatives;

(2) Two appointed by the president pro tempore of the Senate;

(3) One appointed by the majority leader of the House of Representatives;

(4) One appointed by the majority leader of the Senate;

(5) One appointed by the minority leader of the House of Representatives;

(6) One appointed by the minority leader of the Senate; and

(7) The chairperson of the Freedom of Information Commission, or his designee.

(c) The members appointed under subdivisions (1) to (6), inclusive, of subsection (b) of this section shall include two certified public accountants, three representatives of businesses and three representatives of public agencies, as defined in section 1-18a of the general statutes, as amended by section 1 of public act 97-47.

(d) The commission shall elect a chairperson and a vice-chairperson from among its members. Any person absent from (1) three consecutive meetings of the commission or (2) fifty per cent of such meetings during any calendar year shall be deemed to have resigned from the commission, effective immediately. Vacancies on the commission shall be

filled by the appointing authority. Members of the commission shall serve without compensation but shall, within the limits of available funds, be reimbursed for expenses necessarily incurred in the performance of their duties. The commission shall meet as often as deemed necessary by the chairperson or a majority of the commission.

(e) The commission shall submit proposed regulations to the Secretary of the State (1) establishing attestation standards for auditing businesses for compliance with the Voluntary Code for the Protection of Personal Information set forth in section 2 of this act, (2) determining the types of entities which may conduct such audits and (3) establishing appropriate fees for in-state and out-of-state businesses seeking certification by the Secretary of the State under section 4 of this act.

(f) The commission may use such funds as may be available from federal, state or other sources and may enter into contracts to carry out the purposes of this section.

(g) The Freedom of Information Commission shall provide staff assistance to the commission.

(h) The Personal Information Standards Commission shall terminate one year after it submits the proposed regulations described in subsection (e) of this section to the Secretary of the State.

Sec. 4. (NEW) (a) The Secretary of the State shall certify any business as complying with the Voluntary Code for the Protection of Personal Information set forth in section 2 of this act, if the business submits to the Secretary of the State a certificate of compliance audit, accompanied by the fee prescribed in regulations adopted by the Secretary of the State pursuant to subsection (b) of this section. A certificate of compliance audit shall verify that (1) an auditing entity described in such regulations has conducted a compliance audit of the personal information practices of a business in accordance with the attestation standards set forth in such regulations and (2) the business is in compliance with the Voluntary Code for the Protection of Personal Information.

(b) The Secretary of the State shall adopt regulations, in accordance with the provisions of chapter 54 of the general statutes, (1)

incorporating the proposed regulations submitted to the Secretary of the State by the Personal Information Standards Commission pursuant to section 3 of this act, and (2) establishing application procedures for certifications issued by the Secretary of the State pursuant to subsection (a) of this section and procedures for decertifying any certified business which subsequently fails to comply with the provisions of section 2 of this act.

Sec. 5. Not later than October 1, 2000, the Secretary of the State shall submit a report on the implementation of the provisions of sections 1 to 4, inclusive, of this act, including any recommended amendments to said sections, to the joint standing committee of the General Assembly having cognizance of matters relating to government administration.

GAE COMMITTEE VOTE: YEA 12 NAY 5 JF

* * * * *

"THE FOLLOWING FISCAL IMPACT STATEMENT AND BILL ANALYSIS ARE PREPARED FOR THE BENEFIT OF MEMBERS OF THE GENERAL ASSEMBLY, SOLELY FOR PURPOSES OF INFORMATION, SUMMARIZATION AND EXPLANATION AND DO NOT REPRESENT THE INTENT OF THE GENERAL ASSEMBLY OR EITHER HOUSE THEREOF FOR ANY PURPOSE."

* * * * *

FISCAL IMPACT STATEMENT - BILL NUMBER HB 5394

STATE IMPACT	Cost, Can Be Absorbed Within Anticipated Resources, Workload Increase, see explanation below
MUNICIPAL IMPACT	None
STATE AGENCY(S)	Secretary of State, Freedom of Information Commission

EXPLANATION OF ESTIMATES:

Passage of this bill will result in a workload increase to the Secretary of State's Office and the Freedom of Information Commission which can be handled within the anticipated budgetary resources of each agency. The workload increase is dependent upon the number of businesses that pursue voluntary certification.

It is anticipated that there may be costs for the Secretary of State's Office (SOS) for necessary computer modifications and administrative review of the certification requirements, which will be offset by fees collected from businesses seeking voluntary certification for the protection of personal information.

The Freedom of Information Commission will provide staff support to the Personal Information Standards Commission, established by this bill, which will result in an increased workload to the Freedom of Information Commission. The Personal Information Standards Commission will incur costs, which are to be funded through available state and federal funds. The sources of these funds have not been identified. Consultants may be hired to assist the commission in establishing

certification standards for auditing business' compliance, determining the types of entities that may perform such audits, and establishing appropriate fees for businesses seeking certification from the Secretary of State.

Establishing a voluntary business code for the protection of personal information will require the Secretary of State (SOS) to have increased administrative duties, including issuing certificates to those businesses in compliance, establishing de-certification procedures, adopting regulations, and issuing a report and recommendations to the legislature. However, it is not the SOS' responsibility to develop these standards or certify a business' compliance with such standards. Rather the Personal Information Standards Commission develops such standards including provisions for independent audit compliance and the SOS adopts the necessary regulations for these standards, and issues certificates to those companies who have complied with the standards set by the Personal Information Standards Commission.

Businesses seeking voluntary certification will hire an authorized audit entity to certify compliance and the business shall submit such an audit to the Secretary of State. Depending upon the number of business seeking such voluntary certification, there will be a workload increase to the SOS. Additionally, since sole proprietors are eligible for such voluntary certification, the SOS may incur a minimal cost to modify their computers system to accommodate these types of businesses not previously tracked, however it is anticipated that the SOS will be charging fees sufficient to offset these costs.

* * * * *

OLR BILL ANALYSIS

HB 5394

AN ACT ESTABLISHING A VOLUNTARY BUSINESS CODE FOR THE PROTECTION OF PERSONAL INFORMATION

SUMMARY: This bill establishes a Voluntary Code for the Protection of Personal Information. Under the bill, the secretary of the state (SOS) (1) certifies businesses

that volunteer to comply with the code's provisions on the collection, maintenance, use, dissemination, and accuracy of personal information; (2) establishes decertification procedures; (3) adopts regulations; and (4) by October 1, 2000, gives a code implementation report, including recommendations for amendments, to the Government Administration and Elections Committee.

The bill establishes a nine-member Personal Information Standards Commission to draft proposed regulations that specify standards for compliance audits, the types of businesses that may conduct the audits, and the certification fees. The commission must submit these proposed regulations to the SOS who must incorporate them in the regulations he adopts. The commission terminates one year after it completes its responsibilities.

EFFECTIVE DATE: October 1, 1998

FURTHER EXPLANATION

Voluntary Personal Information Protection Code

The SOS may certify a business organization or entity that chooses to comply with the code's principles on collecting, maintaining, correcting, and disclosing personal information. Public agencies and individuals who are not sole proprietors are not eligible for certification. "Personal information" is recorded information that identifies a person in a variety of different ways, including by race, marital or family status, medical history, an identifying number or symbol, fingerprints, or blood type.

Consent. Generally, certified businesses must agree to get consent before collecting, using, or disclosing personal information. Consent is not required if:

1. legal, medical, or security reasons make it impossible or impractical;

2. it defeats fraud or law enforcement detection or prevention efforts;

3. it is impossible or inappropriate because the subject is a minor, seriously ill, or mentally incapacitated;

4. the business has not had a direct relationship with the subject;

5. the law authorizes nonconsensual collection, use, or disclosure or a subpoena, court order, or other judicial process requires it;

6. nonconsensual collection, use, or disclosure is necessary to perform a contract where the subject is a party or to take steps at the subject's request before entering a contract;

7. collection, use, or disclosure is necessary to protect the subject's vital interests or to perform a task that is in the public's interest; or

8. collection, use, or disclosure furthers a legitimate business interest, except when such (a) information reveals a subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, health, or sex life; or (b) interests are overridden by a subject's fundamental rights and freedoms, particularly his right to privacy.

Identifying Purpose. Upon the written request of the subject of information or the person providing it, certified businesses must provide their intended purpose for collecting, using, or disclosing it. Businesses are not required to state the purpose if a third party supplied the information and identifying the purpose is either impossible or would involve a disproportionate effort.

Objections to Collection, Use, or Disclosure. Businesses must allow people from whom or about whom information is collected the right to object to its collection, use, or disclosure at any time and on compelling legitimate grounds relating to the person's particular situation.

Maintaining Personal Information. Once they collect personal information, certified businesses must agree to:

1. inform their employees who operate, keep, or

have access to records containing personal information of the code's provisions, the business' procedures, and any applicable laws or regulations regarding maintenance or disclosure of such information;

2. designate at least one person to be accountable for code compliance and provide that person's name to anyone who asks for it;

3. be responsible for personal information under their control or possession, including when it is transferred for third party processing;

4. protect the information from fire, flood, natural disaster, other physical threats, theft, loss, unauthorized access, disclosure, copying, modification, and use;

5. destroy, erase, or make anonymous information that is no longer needed to fulfill the identified purpose;

6. maintain information only if it is relevant and necessary to accomplish the purposes they identified at or before collection;

7. make their personal information management policies and practices readily available; and

8. upon written request, tell people in writing if the business maintains personal information about them and disclose it on an easily read form, except detrimental medical or psychiatric information and legally withheld information need not be disclosed.

Maintaining Accurate Information. Each certified business must establish procedures for the subject of information to challenge its accuracy, including allowing him to make corrections if the business concurs or add to the business' records a permanent statement of personal information he believes is correct.

Disclosure. When information is disclosed and a person from whom or about whom personal information is collected has requested in writing, the business must

tell him (1) the recipient's identity, (2) whether the disclosure was obligatory or voluntary, (3) the possible consequences for failing to disclose, and (4) his right to access and correct the information. This provision does not apply if a third party provided the information and making the disclosures required under this section is impossible or would involve a disproportionate effort.

Personal Information Standards Commission

The bill requires the Personal Information Standards Commission to draft proposed regulations (1) establishing attestation standards for auditing businesses' code compliance, (2) determining the types of entities that may conduct the audits, and (3) establishing appropriate fees for businesses seeking certification. The commission must submit the proposed regulations to the SOS. It may use available funds from any source, including federal and state, and enter into contracts to carry out its purposes.

The commission must consist of the following members:

1. two each appointed by the Senate president pro tempore and the House speaker,

2. one each appointed by the Senate and House majority leaders,

3. one each appointed by the Senate and House minority leaders, and

4. the Freedom of Information Commission (FOIC) chairperson or his designee.

The appointed members must include two certified public accountants, three business representatives, and three public agency representatives. Commission members serve without pay but must be compensated for necessary expenses from available funds. The FOIC must provide staff assistance.

The commission must elect a chairperson and vice-chairperson from its members and meet as often as the chair or a majority of its members deem necessary. Anyone absent from three consecutive meetings or 50% of the meetings during a calendar year is deemed to have

resigned and the appointing authority must fill the vacancy.

SOS Certifying Businesses

The SOS must adopt regulations (1) incorporating the commission's proposed regulations and (2) establishing application and decertification procedures for businesses that comply or subsequently fail to comply with the code.

He must certify any business that gives him a certificate of compliance audit and pays the appropriate fee. The certificate of compliance must verify that (1) an auditing entity conducted a compliance audit of the business' personal information practices in accordance with the attestation standards provided in the regulations and (2) the business is in compliance with the voluntary code.

COMMITTEE ACTION

Government Administration and Elections Committee

Joint Favorable Report
Yea 12 Nay 5